REMARKS

Upon entry of the present amendment, claims 1, 9 and 10 will be amended, and claims 28-31 will be newly added. Claims 1-31 will remain pending in the present application. Claims 1, 10, 15 and 21 are independent claims.

Applicant respectfully submits that the amendments to the claims are fully supported by the original disclosure, and introduce no new matter therewith. Applicant requests reconsideration and allowance in view of the foregoing amendments and the following remarks.

Consideration of the IDS filed on March 28, 2006 is respectfully requested.

Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold and Fischer

Claims 1-9 and 15-18 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schneier (pages 166, 167, 176 and 177 of Applied Cryptography) in view of Ober (U.S. Patent No. 6,307,936), Arnold (U.S. Patent No. 6,175,924) and Fischer (U.S. Patent No. 6,141,423). Applicant respectfully traverses this rejection.

Applicant respectfully submits that for at least the following two reasons, the combined teachings of Schneier, Ober, Arnold and Fischer do not establish a *prima facie* case of obviousness to reject amended claim 1 and claim 15.

Section 8.3 of Schenier whimsically describes Alice's problems in transferring securely a key she generated to Bob. None of the methods described (meeting Bob in a back alley, using alternate secure channels, a trusted messenger, splitting the key into several different parts and sending each part over a different channel, etc.) appear to correspond to the method steps of claim 1.

If Alice and Bob had the system required to perform the method of claim 1, Bob would already have a secure module, a processor executing a program, and a second super-root key making it possible for Alice to send the encrypted key over an insecure channel.

According to Claim 1, the key provider (corresponding to Alice) has two keys in her possession, a first root key and a first super-root key used to encrypt the first root key. The "second other system" (Bob's) includes a first secure module containing a second super-root key accessible only by a program code executed on a processor located in the secure module. In the claimed method, the encrypted first root key is transferred by the key provider over an insecure link to the processor in the secure module of the "second other system" where it is decrypted using the second super-root key. The decrypted first root key can then used for encrypting and decrypting private keys.

The last paragraph on page 176 of Schenier states "The X9.17 standard specifies two types of keys: key encryption keys and data keys.....These key-encrypting keys have to be distributed manually (although they can be secured in a tamperproof device, like a smart card), but only seldomly." It is not seen that Schenier teaches the claimed method in which the "second other system" is provided with a secure module containing a second super-root key and a processor which, using the program code and the second super-root key, decrypts the encrypted first root key transmitted by the provider.

Furthermore, as previously argued, Schneier, Arnold and Fischer do not teach or reasonably suggest the claimed relationship between the "first root key," the "first super-root key," and the "private encryptions keys." Specifically, Schneier, Arnold and Fischer do not teach or reasonably

suggest "encrypting the **first root key** using **a first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root key** is useable for at least one of encrypting and decrypting **private keys**," as recited in claim 1. Schneier only discloses two types of keys: Key-Encryption Keys and Data Keys, and therefore does not teach a relationship between three keys (see Schneier, page 176). Arnold only discloses two types of keys: the private key K_{PR} and the public key K_{PU}, and thus does not teach a relationship between three keys (see Arnold, col. 5, lines 31-38). Fischer discloses a private key, a random DES key, a public key, and a trustee's public key (see Fischer, col. 4, lines 59-61, col. 7, lines 28-33, col. 9, lines 58-60). However, Fischer does not teach or suggest encrypting the random DES key with the public key, transferring the encrypted random DES key to a key provider to a second system via an information network, and using the random DES key for encrypting and decrypting the private key. Thus, Schneier, Arnold and Fischer do not teach or reasonably suggest "encrypting the **first root key** using **a first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root key** is useable for at least one of encrypting and decrypting **private keys**," as recited in claims 1 and 15.

Ober fails to supplement the deficiencies of Schneier, Arnold and Fischer because Ober does not teach or reasonably suggest not teach or reasonably suggest "encrypting the **first root key** using **a first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root key** is useable for at least one of encrypting and decrypting **private keys**," as recited in claims 1 and 15.

Second, the Office has improperly applied individual parts of Schneier, Ober, Arnold and Fischer as a mosaic to recreate a facsimile of the invention. It is well known that it is improper to use the claims as a frame, and use individual parts of prior art as a mosaic to recreate a facsimile of the invention. *Interconnect Planning Corp. v. Feil*, 227 USPQ 2d 543, 551 (Fed. Cir. 1985).

Schneier, Ober, Arnold, Fischer, or any combination thereof fails to render claim 1 or claim 15 unpatentable under 35 U.S.C. § 103(a) because in order to establish a *prima facie* case of obviousness, all of the claimed limitations must be taught or suggested by the prior art, and there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or to combine the reference teachings. *In re Vaek*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). The application of Schneier, Ober, Arnold and Fischer by the Office fails to meet this criteria, and claims 1 and 15 are allowable over Schneier, Ober, Arnold and Fischer.

Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold, Fischer and Spelman

Claims 10-14 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schneier (pages 166, 167, 176 and 177 of Applied Cryptography) in view of Ober (U.S. Patent No. 6,307,936), Arnold (U.S. Patent No. 6,175,924), Fischer (U.S. Patent No. 6,141,423) and Spelman (U.S. Patent No. 5,680,458). Applicant respectfully traverses this rejection.

Amended claim 10 recites a method for transferring a first root key between a key provider system and a second other system via an information network. The method includes the steps of a) encrypting the first root key using a first super-root key of the key provider system; b) providing

within the second other system a first secure module having second and third super-root keys within a memory circuit thereof, the second and third super-root keys accessible only by program code being executed on a processor internal to the first secure module for decrypting encrypted root keys and for storing the decrypted root keys within a memory circuit of the first secure module, and wherein the second and third super-root keys are other than accessible outside of the module; c) transferring the encrypted first root key from the key provider system to the second other system via the information network; d) providing the encrypted first root key to the processor internal to the first secure module of the second other system; and, e) executing program code on the processor internal to the first secure module to decrypt the encrypted first root key using the second super-root key stored within the memory circuit of the first secure module and to store the decrypted first root key internally within a secure key memory location of the first secure module, wherein the first root key is useable for at least one of encrypting and decrypting private keys, and wherein a bit length of the first super-root key is greater than a bit length of the first root key, and the bit length of the first root key is greater than a bit length of any of the private keys.

Claim 10 is allowable for reasons analagous to those given for claims 1 and 15.

Further, Spelman describes a root key compromise recovery. Spelman fails to supplement the deficiencies of Schneier, Ober, Arnold and Fischer because Spelman fails to teach or reasonably suggest "encrypting the **first root key** using **a first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root key** is useable for at least one of encrypting and decrypting **private keys**," as recited in claim 10.

Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold, Fischer and Easter

Claim 19 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schneier (pages 166, 167, 176 and 177 of Applied Cryptography) in view of Ober (U.S. Patent No. 6,307,936), Arnold (U.S. Patent No. 6,175,924), Fischer (U.S. Patent No. 6,141,423) and Easter (U.S. Patent No. 5,598,889). Applicant respectfully traverses this rejection.

Additional features of the invention recited in claim 18 are found in dependent claim 19.

Claim 19 recites that the module is FIPS 140 compliant.

Claim 19 is allowable for at least the same reasons given above with respect to claim 18 and for the additional features recited therein.

Further, Easter describes a system and method for data encryption using public key cryptology. Easter fails to supplement the deficiencies of Schneier, Arnold and Fischer because Fischer does not teach or reasonably suggest not teach or reasonably suggest "encrypting the **first root key** using **a first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root key** is useable for at least one of encrypting and decrypting **private keys**," as recited in claim 15.

Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 19 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold, Fischer and Easter.

Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold, Fischer and Bergum

Claim 20 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schneier (Applied Cryptography) in view of Ober (U.S. Patent No. 6,307,936), Arnold (U.S. Patent No. 6,175,924), Fischer (U.S. Patent No. 6,141,423), Easter (U.S. Patent No. 5,598,889) and Bergum (U.S. Patent No. 5,249,277). Applicant respectfully traverses this rejection.

Additional features of the invention recited in claim 19 are found in dependent claim 20.

Claim 20 recites that the module includes a tamper detection circuit for erasing the first super-root key in dependence upon a detected attempt to access the electronic contents of the module in an unauthorized fashion.

Claim 20 is allowable for at least the same reasons given above with respect to claim 19 and for the additional features recited therein.

Further, Bergum describes a method and apparatus of controlling processing devices during power transitions. Bergum fails to supplement the deficiencies of Schneier, Ober, Arnold, Fischer, and Easter because Bergum fails to teach or reasonably suggest "encrypting the **first root key** using **a first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root key** is useable for at least one of encrypting and decrypting **private keys**," as recited in claim 15.

Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 20 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold, Fischer, Easter and Bergum.

Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold, Fischer, Mason and Ehrsam

Claims 21-24 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schneier (pages 166, 167, 176 and 177 of Applied Cryptography) in view of Ober (U.S. Patent No. 6,307,936), Arnold (U.S. Patent No. 6,175,924), Fischer (U.S. Patent No. 6,141,423), Spelman (U.S. Patent No. 5,680,458) and Mason (U.S. Patent No. 6,331,784). Applicant respectfully traverses this rejection.

Claim 21 is allowable for reasons analagous to those given for claims 1, 10 and 15.

Further, Spelman describes a root key compromise recovery and Bergum describes a method and apparatus of controlling processing devices during power transitions. Spelman and Bergum fail to supplement the deficiencies of Schneier, Ober, Arnold and Fischer because Spelman and Bergum fail to teach or reasonably suggest "encrypting the **first root key** using **a first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root key** is useable for at least one of encrypting and decrypting **private keys**," as recited in claim 15.

Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold, Fischer, Mason, Ehrsam and Easter

Claim 25 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schneier (pages 166, 167, 176 and 177 of Applied Cryptography) in view of Ober (U.S. Patent No. 6,307,936), Arnold (U.S. Patent No. 6,175,924), Fischer (U.S. Patent No. 6,141,423), Spelman (U.S. Patent No. 5,680,458), Mason (U.S. Patent No. 6,331,784) and Ehrsam (U.S. Patent No. 4,386,234). Applicant respectfully traverses this rejection.

Additional features of the invention recited in claim 24 are found in dependent claim 25.

Claim 25 recites that the substantially non-volatile reprogrammable memory circuit is one of an electrically erasable programmable read-only memory (EEPROM) circuit and a random access memory (RAM) circuit having an on-board power supply in the form of a battery.

Claim 25 is allowable for at least the same reasons given above with respect to claim 24 and for the additional features recited therein.

Further, Ehrsam describes a cryptographic communication and file security using terminals. Ehrsam fails to supplement the deficiencies of Schneier, Ober, Arnold, Fischer, Spelman and Mason because Ehrsam fails to teach or reasonably suggest "encrypting the **first root key** using **a first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root key** is useable for at least one of encrypting and decrypting **private keys**," as recited in claim 21.

Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 25 under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of Ober, Arnold, Fischer, Spelman, Mason and Ehrsam.

Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold, Fischer, Mason, Ehrsam and Easter

Claim 26 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schneier (pages 166, 167, 176 and 177 of Applied Cryptography) in view of Ober (U.S. Patent No. 6,307,936), Arnold (U.S. Patent No. 6,175,924), Fischer (U.S. Patent No. 6,141,423), Spelman (U.S. Patent No. 5,680,458), Mason (U.S. Patent No. 6,331,784), Ehrsam (U.S. Patent No. 4,386,234) and Easter (U.S. Patent No. 5,598,889). Applicant respectfully traverses this rejection.

Additional features of the invention recited in claim 25 are found in dependent claim 26.

Claim 26 recites that the module is FIPS 140 compliant.

Claim 26 is allowable for at least the same reasons given above with respect to claim 25 and for the additional features recited therein.

Further, Easter describes a system and method for data encryption using public key cryptography. Easter fails to supplement the deficiencies of Schneier, Ober, Arnold, Fischer, Spelman, Mason and Ehrsam because Easter fails to teach or reasonably suggest "encrypting the **first root key** using **a first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root key** is useable for at least one of encrypting and decrypting **private keys**," as recited in claim 21.

Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 26 under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of Ober, Arnold, Fischer, Spelman, Mason, Ehrsam and Easter.

Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold, Fischer, Mason, Ehrsam, Easter and Bergum

Claim 27 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schneier (pages 166, 167, 176 and 177 of Applied Cryptography) in view of Ober (U.S. Patent No. 6,307,936), Arnold (U.S. Patent No. 6,175,924), Fischer (U.S. Patent No. 6,141,423), Spelman (U.S. Patent No. 5,680,458), Mason (U.S. Patent No. 6,331,784), Ehrsam (U.S. Patent No.

4,386,234), Easter (U.S. Patent No. 5,598,889) and Bergum (U.S. Patent No. 5,249,277). Applicant respectfully traverses this rejection.

Additional features of the invention recited in claim 26 are found in dependent claim 27.

Claim 27 recites that the module includes a tamper detection circuit for erasing every cryptographic key stored within the memory circuit in dependence upon a detected attempt to access the electronic contents of the module in an unauthorized fashion.

Claim 27 is allowable for at least the same reasons given above with respect to claim 26 and for the additional features recited therein.

Further, Bergum describes a system and method for data encryption using public key cryptography. Bergum fails to supplement the deficiencies of Schneier, Ober, Arnold, Fischer, Spelman, Mason, Ehrsam and Easter because Bergum fails to teach or reasonably suggest "encrypting the **first root key** using **a first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root key** is useable for at least one of encrypting and decrypting **private keys**," as recited in claim 21.

Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 27 under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of Ober, Arnold, Fischer, Spelman, Mason, Ehrsam, Easter and Bergum.

The dependent claims not specifically discussed above are patentable at least for the reasons regarding their respective independent claims.

New Claims

Newly added dependent claims 28-31 respectively depend from claims 1, 10, 15 and 21, and are allowable as being dependent from an allowable claim.

Further, each of these claims recites that the bit length of the first super-root key is within an approximate range of between 2048 bits and 4096 bits, the bit length of the first root key is within an approximate range of between 512 bits and 2048 bits, and the bit length of any of the private keys is within an approximate range of between 128 and 1024 bits

Applicant respectfully submits that Schneier, Ober, Arnold, Fischer, Spelman, Mason, Ehrsam, Easter, Bergum, or any combination thereof fails to teach or reasonably suggest these bit ranges.

Conclusion

Applicant respectfully submits that the proposed amendments made herein properly respond to the outstanding Final Rejection and represent a *bona fide* effort to satisfactorily conclude the prosecution of this application. Care has been exercised to insure that no new matter has been introduced and that no new issues have been raised that would require further consideration or search. It is felt that no inordinate amount of time will be required on the part of the Examiner to review and consider this amendment. In the event that the application is not allowed, it is requested that this amendment be entered for purposes of appeal.

All of the stated grounds of rejection have been properly traversed. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding rejections and that they

be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is hereby invited to telephone the undersigned at the number provided.

No additional fees are believed to be required. However, if the Office deems that any fees are necessary, authorization is hereby granted to charge any required fees to Deposit Account No. 22-0261.

Prompt and favorable consideration of this Amendment is respectfully requested.

In view of the above amendment, applicant believes the pending application is in condition for allowance.

Dated: July 28, 2006

Respectfully submitted,

By _____

Jeffri A. Kaminski
Registration No.: 42,709
James R. Burdett
Registration No.: 31,594
VENABLE LLP
P.O. Box 34385
Washington, DC 20043-9998
(202) 344-4000
(202) 344-8300 (Fax)
Attorney/Agent For Applicant